УДК 519.7

М. М. Касянчук, канд. фіз.-мат. наук, доцент,
І. З. Якименко, канд. техн. наук,
С. В. Івасьєв, канд. техн. наук,
Б. О. Маслияк, канд. техн. наук, доцент

Тернопільський національний економічний університет, м. Тернопіль

МЕТОД РОЗШИРЕННЯ НАБОРУ МОДУЛІВ МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

У роботі представлений метод розширення набору модулів модифікованої досконалої форми системи залишкових класів. Показано, що в залежності від їх вибору розрядність чисел, над якими виконуватимуться арифметичні операції, зменшується в 2–3 рази. Це особливо актуально при обчисленнях з багаторозрядними числами.

Ключові слова: *система залишкових класів, модифікована досконала форма, розширення набору модулів.*

Вступ. Найперспективнішим шляхом підвищення швидкодії сучасних обчислювальних систем є розпаралелення процесу обробки інформації [1]. Цією властивістю володіють деякі непозиційні системи числення, зокрема система залишкових класів (СЗК) [2]. Її успішно можна застосовувати для додавання, віднімання, піднесення до степеня, множення цілих багаторозрядних чисел [3], що є дуже важливим, зокрема, у асиметричній криптографії [4], розробці нових засобів та алгоритмів завадозахищеного кодування [5], для підвищення достовірності контролю даних [6], при великих матричних обчисленнях [7], інших задачах прикладної та дискретної математики [8].

Аналіз літературних джерел. Будь-яке ціле десяткове число N в СЗК представляється у вигляді набору $(b_1, b_2, \ldots, b_n)$ найменших додатних залишків від ділення цього числа на фіксовані натуральні попарно взаємно прості числа $p_1, p_2, \ldots, p_n$ ($b_i = N \bmod p_i$), які називаються модулями (n — кількість модулів). При цьому повинна виконуватися нерівність $0 \le N < P - 1$, де $P = \prod_{i=1}^{n} p_i$ — число, що визначає умову переповнення розрядної сітки.

Зворотне перетворення із СЗК у десяткову систему числення грунтується на використанні китайської теореми про залишки [9] і є досить громіздким процесом:

$$N = \left(\sum_{i=1}^{k} b_i B_i \right) \bmod P , \qquad (1)$$

де $B_i = M_i m_i$, $M_i = \dfrac{P}{p_i}$, $m_i = M_i^{-1} \bmod p_i = 1$.

Всі відомі методи пошуку оберненого елемента характеризуються значною обчислювальною складністю, вимагають великих затрат часових та апаратних ресурсів.

У працях [10, 11] описана досконала форма (ДФ) СЗК, в якій виконується умова $M_i \bmod p_i = 1$, що дозволяє уникнути процедури пошуку оберненого елемента і множення на нього в (1). У роботі [12] вирішена задача та визначені умови для аналітичного знаходження m_i. Однак в обох випадках значення p_i швидко збільшуються, що неприпустимо при необхідності використання модулів однакової розрядності. В роботах [13, 14] розроблені теоретичні основи модифікованої досконалої форми (МДФ) СЗК, у якій виконується така рівність:

$$M_i \bmod p_i = \pm 1, \tag{2}$$

що також усуває операцію пошуку оберненого елемента. Однак на даний час відсутні методи розширення системи модулів, які також задовольняють умовам МДФ СЗК.

В роботі [10] отримано вираз для пошуку набору модулів ДФ СЗК. Аналогічні міркування приводять до умови, яка має виконуватися для МДФ СЗК:

$$\sum_{i=1}^{n} \frac{1}{p_i} = k \pm \frac{1}{\prod_{i=1}^{n} p_i}. \tag{3}$$

У відомих методах пошуку модулів МДФ СЗК приймалося, що $k = 0$, однак даний параметр може набувати інших цілих значень ($k = \pm 1, \pm 2, \pm 3, \ldots$). Тому метою роботи є розробка методу розширення набору модулів МДФ СЗК при будь-якому цілому значенні параметра *k*.

Метод розширення модифікованої досконалої форми системи залишкових класів. Для демонстрації методу та спрощення розрахунків обмежимо наші міркування п'ятьма модулями, перші три з яких утворюють ДФ СЗК. Єдиним можливим варіантом є набір $p_1 = 2, p_2 = 3, p_3 = 5$. Тоді вираз (3) набуде такого вигляду:

$$\frac{31}{30} + \frac{1}{p_4} + \frac{1}{p_5} = k \pm \frac{1}{30 p_4 p_5}. \tag{4}$$

Після відповідних математичних перетворень (4) трансформується в таку умову:

$$(31 - 30k) p_4 p_5 + 30(p_4 + p_5) = \pm 1. \tag{5}$$

На рис. 1 показаний графік залежності p_5 від p_4 при $k=1$. З нього видно, що при $p_4<-30$ та $p_4>1/30$ модуль p_5 набуває від'ємних значень, в інших випадках модуль p_5 додатній.

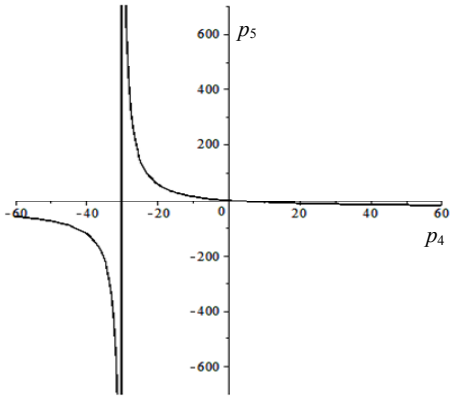

Рис. 1. *Графік залежності* p_5 *від* p_4 *при* $k=1$

Ввівши заміну $p_{4,5}=\dfrac{a,b-30}{31-30k}$, отримаємо вираз для цілочисельного розв'язку (10): $ab=\pm(31-30k)+30^2$.

Розглянемо різні значення параметра *k*.

1) $k=0$. Тоді $ab=\pm31+30^2=\begin{cases}931=7\cdot7\cdot19\\869=11\cdot79.\end{cases}$

В табл. 1 наведено усі можливі цілочисельні значення *a* та *b*, які визначаються факторизацією, а також випадки, коли існують набори модулів МДФ СЗК та діапазон відповідних обчислень.

З табл. 1 видно, що розрядність чисел, над якими виконуються арифметичні операції, зменшується приблизно вдвічі. Значення $p_4=-1$ вказує на те, що набори з чотирьох модулів 2, 3, 5, 29 та 2, 3, 5, 31 утворюють МДФ СЗК, у яких кожен наступний модуль на одиницю відрізняється від добутку попередніх. Крім того, у восьми з десяти можливих випадків, що утворюються при факторизації, цілочисельних наборів модулів не існує.

2) $k=1$. Тоді $ab=\pm1+30^2=\begin{cases}901=17\cdot53\\899=29\cdot31.\end{cases}$ При даній умові будь-яким значенням *a* та *b* відповідатимуть цілочисельні модулі p_4 та p_5. Результати наведено в табл. 2.

Таблиця 1

Можливі варіанти систем з п'яти модулів для МДФ СЗК при $p_1 = 2, p_2 = 3, p_3 = 5$ *та* $k = 0$ (*в дужках — розрядність у двійковій системі числення*)

№	*ab*	*a*	*b*	p_4	p_5	*P*
1	869	1	869	не існує		
2		–1	–869	–1	–29 (5)	870 (10)
3		11	79	не існує		
4		–11	–79	не існує		
5	931	1	931	не існує		
6		–1	–931	–1	–31 (5)	930 (10)
7		7	133	не існує		
8		–7	–133	не існує		
9		19	49	не існує		
10		–19	–49	не існує		

Таблиця 2

Можливі варіанти систем з п'яти модулів для МДФ СЗК при $p_1 = 2, p_2 = 3, p_3 = 5$ *та* $k = 1$ (*в дужках — розрядність у двійковій системі числення*)

№	*ab*	*a*	*b*	p_4	p_5	*P*
1	899	1	899	–29 (5)	869 (10)	756030 (20)
2		–1	–899	–31 (5)	–929 (10)	863970 (20)
3		29	31	–1 (1)	1 (1)	30 (5)
4		–29	–31	–59 (6)	–61 (6)	107970 (17)
5	901	1	901	–29 (5)	871 (10)	757770 (20)
6		–1	–901	–31 (5)	–931 (10)	865830 (20)
7		17	53	–13 (4)	23 (5)	8970 (14)
8		–17	–53	–47 (6)	–83 (7)	117030 (17)

Табл. 2 показує, що розрядність чисел, над якими виконуються арифметичні операції, зменшується приблизно в 2–3 рази. Третій рядок таблиці вказує, що модулі 2, 3, 5 утворюють ДФ СЗК. Модуль p_4 завжди від'ємний, знак модуля p_5 збігається із знаком параметрів *a* та *b*, причому в цьому випадку $p_4 > -30$, що узгоджується з графіком на рисунку 1. Найбільший діапазон обчислень буде в тому випадку, коли абсолютна величина кожного наступного модуля на одиницю більша від добутку абсолютних величин попередніх модулів.

Чисельні розрахунки показують, що при інших значеннях параметра *k* отримані модулі відрізнятимуться від знайдених при $k = 0,\ 1$ лише знаком. Для проведення подальших досліджень розподілу абсолютних величин усіх отриманих наборів модулів їх потрібно перенумерувати в порядку зростання $|p_4|$, що представлено у табл. 3.

Таблиця 3

Впорядкування модулів по зростанню $|p_4|$ *при* $p_1 = 2, p_2 = 3, p_3 = 5$

№	1	2	3	4	5	6	7	8	9	10
p_4	1	1	1	13	29	29	31	31	47	59
p_5	1	29	31	23	869	871	929	931	83	61

На рис. 2 показаний характер зміни значень модулів p_4 та p_5 в залежності від номера модуля згідно таблиці 3 у логарифмічній шкалі, не враховуючи значення $p_4 = 1$.

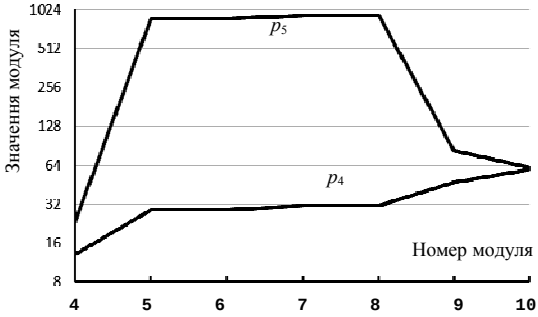

Рис. 2. *Характер зміни значень модулів* p_4 *та* p_5 *при* $p_1 = 2, p_2 = 3, p_3 = 4$ *в залежності від номера модуля згідно табл. 3*

Як видно з рис. 1, значення $|p_4|$ відносно повільно зростає. Водночас, графік для $|p_5|$ зростає набагато інтенсивніше, доходить до плоского максимуму, а потім спадає до значення $|p_4|$.

Висновки. У роботі представлений метод розширення набору модулів модифікованої досконалої форми системи залишкових класів. Показано, що в залежності від їх вибору розрядність чисел, над якими виконуватимуться арифметичні операції, зменшується в 2–3 рази. Встановлено, що найбільший діапазон обчислень при заданих першому модулю та їх кількості буде тоді, коли абсолютні величини всіх наступних модулів на одиницю більші від добутку абсолютних величин попередніх.

Список використаних джерел:

1. Николайчук Я. М. Теорія джерел інформації. Тернопіль: ТзОВ «Терно-граф», 2010. 536 с.
2. Omondi A., Premkumar B. Residue number systems: theory and implementation. London: Imperial College Press, 2007. 296 p.
3. Kozaczko D., Ivasiev S., Yakymenko I., Kasianchuk M. Vector Module Exponential in the Remaining Classes System. Proceedings of the 2015 IEEE 8th

International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015). Warsaw, Poland. 2015. P. 161–163.
4. Задірака В. К., Олексюк О. С. Комп'ютерна криптологія. Тернопіль, Київ, 2002. 504 с.
5. Yatskiv V., Yatskiv N., Jun Su, Sachenko A., Hu Zhengbing. The Use of Modified Correction Code Based on Residue Number System in WSN. Proceedings of the 7 2013 IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'2013). Berlin, Germany. 2013. Vol. 1. P. 513–516.
6. Krasnobayev V. A., Koshman S. A., Mavrina M. A. A Method of Increasing the Reliability of Verification of Data Represented in a Residue Number System. *Cybernetics and Systems Analysis.* Vol. 50, Issue 6, 2014. P. 969–976.
7. Yakymenko I., Kasyanchuk M., Nykolajchuk Ya. Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis. Proceedings of the X-th International Conference *«Modern Problems of Radio Engineering, Telecommunications and Computer Science»* (TCSET–2010). L'viv ; Slavske. 2010. P. 241.
8. Задірака В. К., Олексюк О. С. Комп'ютерна арифметика багаторозрядних чисел. К.: 2003. 264 с.
9. Бухштаб А. А. Теория чисел. М.: Просвещение, 1966. 384 с.
10. Kasianchuk M., Yakymenko I., Pazdriy I., Zastavnyy O. Algorithms of findings of perfect shape modules of remaining classes system. Proceedings of the XIII International Conference *«The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)»*, 23-25 February, 2015, Polyana-Svalyava (Zakarpattya), Ukraine. 2015. P. 168–171.
11. Kasyanchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application. Proceedings of the 4th International Conference *«Advanced Computer Systems and Networks: Design and Application»* (ACSN–2009), Lviv (Ukraine). 2009. P. 299–301.
12. Nykolaychuk Ya. M., Kasianchuk M. M., Yakymenko I. Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. *Cybernetics and Systems Analysis.* Vol. 50, Issue 5, 2014. P. 649–654.
13. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical Foundations of the Modified Perfect Form of Residue Number System. *Cybernetics and Systems Analysis.* Vol. 52, Issue 2, 2016. P. 219–223.
14. Kasianchuk M.N., Nykolaychuk Y.N., Yakymenko I.Z. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes. *Journal of Automation and Information Sciences*. 2016. Vol.48, N 8. P. 56–63.

Present work declaring the method of expansion set of modules of modified perfect form of residual classes' system. It was shown that depends on their choice the bit of numbers, arithmetic operations performed over-their, was reduced by 2–3 times. This is especially necessary in the calculation of multi-digital numbers.

Key words: *system of residual classes, modified perfect form, the expansion set of module.*

Одержано 16.02.2017